

Claims:

- 1 1. An apparatus comprising:
2 Management Frames utilized in wireless communications associated
3 with said apparatus; and
4 said Management Frames being protection-capable or non-protection-
5 capable and wherein said Management Frames indicate whether or not they are
6 protection-capable.
- 1 2. The apparatus of claim 1, wherein at least one of said Management
2 Frames is an Action Frame.
- 1 3. The apparatus of claim 2, wherein said wireless communications
2 further comprises a Robust Security Network (RSN) Capabilities bit to be added for
3 Action Frame protection negotiation.
- 1 4. The apparatus of claim 3, wherein said Action Frame protection
2 negotiation is provided by a Beacon/Probe Response source setting said RSN bit to
3 indicate that protection is required for all protection-capable Action Frames.
- 1 5. The apparatus of claim 3, wherein if said RSN Capabilities bit is set to
2 protection-capable, said Action Frames may be protected by applying the IEEE

3 802.11i CCMP protocol construction to said protection-capable Action Frames.

1 6. The apparatus of claim 3, wherein if said RSN Capabilities bit is set to
2 protection-capable, said Action Frames may be protected by applying the IEEE
3 802.11i TKIP protocol construction to said protection-capable Action Frames.

1 7. The apparatus of claim 5, wherein said CCMP protocol uses CCM to
2 encrypt the Management Frame payload and to protect selected Management
3 Frame header fields from modification.

1 8. The apparatus of claim 5, wherein said apparatus is a pair of wireless
2 stations (STA).

1 9 The apparatus of claim 8, wherein at least one of said pair of wireless
2 stations (STA) is an access point (AP).

1 10. The apparatus of claim 6, wherein said TKIP protocol uses RC4 to
2 encrypt the Management Frame payload and uses Michael to protect selected
3 Management Frame header fields from modification.

1 11. The apparatus of claim 6, wherein said apparatus is a pair of wireless
2 stations (STA).

1 12 The apparatus of claim 11, wherein at least one of said wireless
2 stations (STA) is an access point (AP).

1 13. The apparatus of claim 8, wherein said STA sourcing Beacons and
2 Probe Responses sets to 0 if said protected Action Frames are not
3 supported/enabled; said STA sets to 1 if said protected Action Frames supported
4 and enabled; said responding STA sets to 0 if it doesn't support protected Action
5 Frames; and said responding STA sets to the value set by said sourcing STA if it
6 supports protected Action Frames.

1 14. The apparatus of claim 1, wherein said wireless communications is an
2 802.11 wireless LAN.

1 15. A method of protecting Management Frames in wireless
2 communications, comprising:

3 establishing said Management Frames as protection-capable or non-
4 protection-capable; and

5 protecting said Management Frames if said Management Frames are
6 protection-capable.

1 16. The method of claim 15, wherein said step of protecting said
2 Management Frames, comprises:

3 adding a Robust Security Network (RSN) Capabilities bit to said
4 Management Frames for Management Frame protection negotiation, wherein if said
5 RSN Capabilities bit is set to protection-capable, said Management Frames may be
6 protected by applying a protection protocol to said protection-capable Management
7 Frames.

1 17. The method of claim 16, wherein said Management Frame protection
2 negotiation is provided by a Beacon/Probe Response source setting said RSN bit to
3 indicate that protection is required for all protection-capable Action Frames.

1 18. The method of claim 16, wherein said protection protocol is the IEEE
2 802.11i CCMP protocol construction.

1 19. The method of claim 15, wherein at least one of said Management
2 Frames is an Action Frame.

1 20. The method of claim 16, wherein if said RSN Capabilities bit is set to
2 protection-capable, said Management Frames may be protected by applying the
3 IEEE 802.11i TKIP protocol construction to said protection-capable Action Frames.

1 21. The method of claim 18, wherein said CCMP protocol uses CCM to
2 encrypt the Management Frame payload and to protect selected Management

3 Frame header fields from modification.

1 22 The method of claim 20, wherein said TKIP protocol uses RC4 to
2 encrypt the Management Frame payload and uses Michael to protect selected
3 Management Frame header fields from modification.

1 23. The method of claim 15, wherein said wireless communications is
2 wireless communications between a pair of wireless stations (STA), one which
3 might be an access point (AP).

1 24. The method of claim 23, wherein said sourcing STA sets to 0 if said
2 protected Management Frames are not supported/enabled; said sourcing STA sets
3 to 1 if said protected Management Frames are supported and enabled; said STA
4 sets to 0 if it doesn't support protected Management Frames; and said STA sets to
5 value set by said AP if it supports protected Action Frames.

1 25. The method of claim 15, wherein said wireless communications is an
2 802.11 wireless LAN.

1 26. An article comprising a storage medium having stored thereon
2 instructions, that, when executed by a computing platform, establishes, in a
3 wireless communication environment, protection-capable and non-protection-

4 capable Management Frames, said protection-capable Management Frames being
5 protected.

1 27. The article of claim 26 wherein said protection-capable Management
2 Frames being protected are protected by adding a Robust Security Network (RSN)
3 Capabilities bit to said Management Frames for Management Frame protection
4 negotiation, wherein if said RSN Capabilities bit is set to protection-capable, said
5 Management Frames may be protected by applying a protection protocol to said
6 protection-capable Management Frames.

1 28. The article of claim 27, wherein said Management Frame protection
2 negotiation is provided by a Beacon/Probe Response source setting said RSN bit to
3 indicate that protection is required for all protection-capable Action Frames.

1 29. The article of claim 27, wherein said protection protocol is the IEEE
2 802.11i CCMP or TKIP protocol construction.

1 30. The article of claim 26, wherein at least one of said Management
2 Frames is an Action Frame.

1 31. The article of claim 29, wherein said CCMP protocol uses CCM to
2 encrypt the Management Frame payload and to protect selected Management

3 Frame header fields from modification, or uses the TKIP protocol which uses RC4
4 to encrypt the Management Frame payload and Michael to protect selected
5 Management Frame header fields from modification.

1 32. The article of claim 26, wherein said wireless communications is
2 802.11 wireless communications between a pair wireless stations (STA), one of
3 which may be an access point (AP).

1 33. A system to protect Action Frames in Wireless LAN Communications,
2 comprising:
3 a first wireless station (STA); and
4 a second STA in communication with said first STA, said communication
5 includes non-protection-capable Action Frames and protection-capable Action
6 Frames.

1 34. The system of claim 33, wherein if it is desired not to protect Action
2 Frames, then STAs shall send all Action Frames without protection, including all
3 protection-capable Action Frames.

1 35. The system of claim 33, wherein if it is desired to protect Action
2 Frames, then a STA shall protect all protection-capable Action Frames, said
3 protection provided by adding a Robust Security Network (RSN) Capabilities bit to

4 said Action Frames for Action Frame protection negotiation, wherein if said RSN
5 Capabilities bit is set to protection-capable, said Management Frames may be
6 protected by applying a CCMP protocol which uses CCM to encrypt the
7 Management Frame payload and to protect selected Management Frame header
8 fields from modification, or by applying the TKIP protocol which uses RC4 to
9 encrypt the Management Frame payload and Michael to protect selected
10 Management Frame header fields from modification.

1 36. The system of claim 33, where said first STA shall not send
2 protection-capable Action Frames at all if said second STA has not agreed to
3 protection.

1 37. The system of claim 33, if the wireless communication requires
2 protected Action Frames, then said first or said second STA shall discard any
3 unprotected protection-capable Action Frame it receives.

1 38. The system of claim 37, wherein the discard of any unprotected
2 protection-capable Action Frames includes those received before an IEEE 802.11i
3 4-Way Handshake completes.

1 39. The system of claim 33, wherein neither said first or said second STA
2 shall attempt to protect non-protection-capable Action Frames it sends and shall

3 discard any it receives protected.

1 40. The system of claim 33, further comprising a STA in communication
2 with said second STA.